

ADVANCED
WINDOWS

INTRODUCTION

When Windows XP goes wrong, there are numerous methods to try to remedy things. If you're lucky, you won't have cause to call on the Recovery Console, but if all else fails it might be the only way to get an ailing PC back to rude health.

The Recovery Console is not for the faint-hearted. It harks back to the less-than-golden age of non-graphical interfaces, when all interaction with computers took place via text commands. Communicating with a PC in such an archaic way – a method called the command-line interface – can be perplexing. However, aspects of the control offered by Recovery Console over files and folders are unmatched by more common recovery routes such as Safe Mode and System Restore.

So if your PC is in serious trouble, or you just fancy getting your hands dirty (and we do mean really, really dirty), then this article is for you. We'll explain how to get the Recovery Console up and running, and how to use it to take a troublesome Windows XP computer to task.

Simon Edwards
Technical Editor



windows@computershopper.co.uk

Using Windows' Recovery Console

There are several ways of fixing Windows XP when things don't work as they should, but if all else fails you can use the Recovery Console, as Scott Colvey explains

On the whole, Windows XP is reliable. However, it is also an extremely complex software system and, as with anything complicated, things can go wrong. Microsoft's decision to include the System Restore 'roll-back' utility with Windows Me and XP was little more than a tacit acknowledgement by the company that its sprawling operating system could stumble at unforeseen hurdles.

System Restore is undependable. It can sometimes work like a dream, unwinding all manner of mangling to return a PC back to a previous happy state. On other occasions, it may simply report that it has been unable to do the job. If a PC won't start at all, System Restore is of little or no use initially. In such circumstances, Safe Mode can help to get a sickly computer back on its feet so System Restore can run, but if System Restore refuses to work you're back at square one.

If you are attempting to tame a troublesome computer and all else has failed, it may be time to try Recovery Console. However, this is not a tool for the inexperienced or nervous. Recovery Console lets you get under the bonnet of and its various components. Used wisely and cautiously, it can help bring a dead computer back to life, and you'll be glad of it in situations when a PC refuses to start up. However, with great power comes responsibility, and if you choose the Recovery Console path you do so at your own risk. Please don't blame us if Recovery Console fails to bring you joy, or makes things worse.

RECOVERY CONSOLE'S REMIT

Don't think the Recovery Console is a one-stop repair shop for all a PC's ills: it isn't. The Recovery Console's

powers are limited, and can be broken down into four broad categories. The first is file manipulation. You can use the Recovery Console to copy, rename, delete or otherwise replace files and folders. This can come in handy when you want to fix system files or folders you know or suspect to be corrupt or misconfigured.

The second category is device driver and system service management. With the Recovery Console, it is possible to enable or disable various Windows services and device drivers. You might do this to coax a PC into starting up properly. Third, the Recovery Console can work a little black magic to repair areas of the hard disk that may otherwise be inaccessible to the user, such as the part containing the boot sector or the master boot record (MBR). Finally, it is possible to create, format and delete drive partitions using the Recovery Console.

Most of these tasks can be undertaken from within Windows XP itself, but if you can't launch Windows XP you'll have to resort to the command line.

RUNNING RECOVERY CONSOLE

There are a couple of ways to launch the Recovery Console, with a few requirements and caveats. The main requirement is that, to begin with, you'll need the original Windows XP installation CD-ROM or Windows Setup floppy disks. You'll also need an administrator password for the Windows XP installation with which you intend to work. Without these, you cannot continue. If you are reading this article because you need to use the Recovery Console, hunt these items down now, or bear in mind that they will be required for this article to be of any use. If you've forgotten your Windows administrator password, see the 'Recovering a

At your command Recovery Console commands

There are 29 distinct commands available when using the Recovery Console, though not all are terribly useful. The net command, for example, doesn't work, even though the help file suggests otherwise. Here's a rundown of all the commands, with a brief description of each:

attrib	Use with a + or - modifier to change the Read (R), System (S), Hidden (H) or Compressed (C) attributes of files or folders	fixboot	Writes a new partition boot sector on to the specified partition
batch	Execute commands stored in a text file	fixmbr	Repairs the master boot record of the specified disk
bootcfg	Configures or recovers the boot.ini file	format	Use to format (erase) disks
cd (or chdir)	Displays or changes the current directory (also known as the current folder)	help	Displays a list of the commands available from the Recovery Console
chkdsk	Produces a health-check report on a specified drive	listsvc	Lists the PC's available services and drivers
cls	Clears the screen	logon	Logs on to a Windows installation
copy	Copies one file to another location	map	Displays available drives along with the letters assigned to them
del (or delete)	Deletes one or more files or a directory	md (or mkdir)	Creates a new directory
dir	Displays a list of files and directories stored in the current directory	more	Shows the content of a text file
disable	Disables a service or a device driver	net	Pointless, non-functional command
diskpart	Manages hard disk partitions	rd (or rmdir)	Deletes a directory
enable	Enables a service or a device driver	ren (or rename)	Renames a single file or directory
exit	Exits Recovery Console and restarts the computer	set	Displays or sets environment variables
expand	Extracts content from a compressed file	systemroot	Sets the current directory to the systemroot folder
		type	Shows the content of a text file

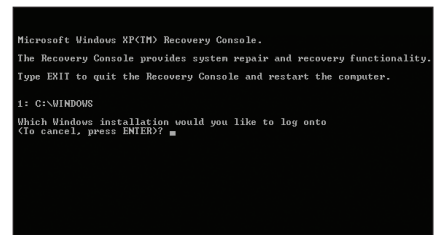
Windows XP administrator password' box on the following page.

The most common way to launch the Recovery Console is to boot from the Windows XP installation disc. To do this, your PC's BIOS must be set up to boot from a CD-ROM. Most modern PCs are set to do this by default, but if yours isn't, or you'd like to check how it is set to boot, look at the basic input/output system (BIOS) settings. Accessing a PC's BIOS usually involves pressing a key soon after the computer has been turned on. The key is Delete or F2. To find out which, read the messages displayed by the PC as it goes through its power-on procedure. These will probably include a prompt explaining how to access the BIOS settings.

Once you've opened the BIOS screen, look for a menu labelled Boot or Startup or an option called 'Boot device priority' or similar. You'll be able to set the order in which your PC tries various devices to start an operating system from. Ensure that the usual boot device, the hard disk, is lower down in the list than the CD-ROM or DVD drive, which we'd recommend putting at the top. Save the settings and exit the BIOS. If you're not sure how, try pressing Esc or F10.

Ensure that the Windows XP installation CD-ROM is in the CD or DVD drive that you put at the top of the boot list. Then power up the computer and wait for a few seconds while the Windows Setup program carries out a few checks. When it's done, it will launch with a blue screen. Press R to run the Recovery Console. If you want, you can add the Recovery Console as a startup option to Windows XP installations. This means it will appear as an option on a menu displayed soon after the PC is powered up. Doing so takes up 7MB of hard disk space and means the Recovery Console will be available whenever required, even if you don't have the Windows XP installation disc to hand.

To set this up, boot into XP as normal. After inserting the Windows XP installation CD into the PC's drive, select Run from the Start menu. Type `d:\i386\winnt32.exe /cmdcons` (where d: is the letter of the drive containing the Windows XP disc) and hit Enter or click OK. Follow the setup wizard's prompts to complete the job, which takes a few seconds. When the PC next reboots, a startup options menu appears complete with a Recovery Console entry. Choose this when you want to run the Recovery Console.



▲ The Recovery Console's opening screen is far from welcoming

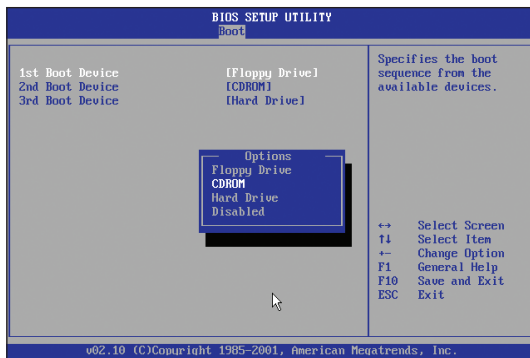
dumped into the Recovery Console at the command-line prompt.

We recommend you type `help` and hit Enter. This displays a list of all the commands available. For detailed help on how to use a particular command, type the command followed by a space and then `/?` or type `help` followed by the command itself. For example, `help chkdsk` shows details about the `chkdsk` utility. See the box opposite for a list of all available commands.

COMMANDS AND TECHNIQUES

As mentioned earlier, the Recovery Console's uses can be divided into four broad categories. Let's begin with file manipulation. For example, to view a list of all available files and folders (known as directories when you're dealing with the command line) in the current directory, type the command `dir` and hit Enter. Press Enter again to scroll through the list one line at a time, or hit the spacebar to skip down a page at a time. When done, press Escape to return to Recovery Console's command line prompt.

Recovery Console starts in the default Windows installation directory, which is usually C:\Windows. To change to a different directory, use the change directory (cd) command. Type cd system and the command-line prompt will change to show that you're in the \Windows\System directory. To get back to the Windows directory, type cd \windows or, to get to the drive's root directory, type cd \. Use the help



▲ You may need to change the device boot order in your PC's BIOS settings to launch the Recovery Console from a Windows XP installation disc

WELCOME TO THE CONSOLE

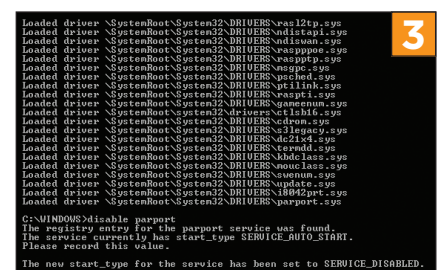
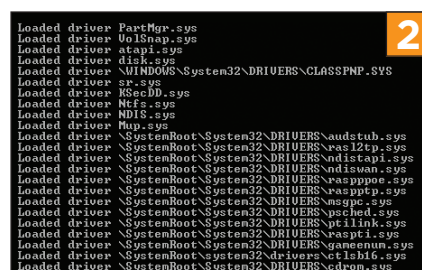
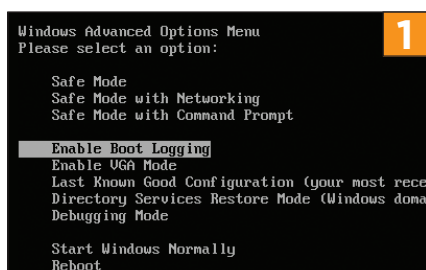
As our screenshot above shows, the Recovery Console's initial screen isn't a pretty sight. What you do next depends on what you want to achieve using Recovery Console. First, you'll need to log on to a Windows XP installation. For many users, this means typing 1 and hitting Enter. If you have a multi-boot system setup, where your PC has two or more operating systems installed on multiple partitions, choose the relevant number from the displayed list. Next, you'll be prompted to type in the administrator password. After you do, you'll be unceremoniously

HOW TO... Disable a device driver or system service

1 To enable boot logging, tap F8 after turning on your computer. When the Windows Advanced Options Menu (pictured in the screenshot below) appears, choose Enable Boot Logging. Select the desired Windows XP installation if given a choice and allow to boot.

as normal, or until the point where the startup grinds to a halt.

2 Enter the Recovery Console and use the `cd` command to switch to the Windows installation directory (usually `C:\Windows`); for



example, `cd windows`. Use the `type` command to display the contents of the log file, called `NTBTLOG.TXT`. Enter `type ntbtlg.txt`.

3 Scroll down to find where the Windows XP startup stalled. Note the name of the last-loaded driver or service. Use Recovery Console's disable command to turn off the suspect driver or service prior to rebooting.

In our example, we typed `disable parport` to prevent Windows XP from launching a service related to the computer's legacy parallel port. Use the `enable` command to re-enable a driver or service.

```

The volume in drive C has no label
The volume Serial Number is 7052-c124

Directory of C:\WINDOWS

01/14/07 02:16p d----- 0 .
01/14/07 02:16p d----- 0 ..
01/14/07 04:20p -a----- 0 0..log
01/11/07 06:45p d----- 0 addins
01/11/07 07:08p d----- 0 appPatch
08/29/02 01:00p -a----- 1222 Blue Lace 16.bmp
01/14/07 04:23p -a-s----- 2048 bootstat.dat
01/12/07 05:46p d----- 0 bun
08/29/02 01:00p -a----- 82944 clock.avi
08/29/02 01:00p -a----- 17062 Coffee Bean.bmp
01/12/07 12:00p -a----- 15718 consetup.log
01/11/07 06:45p d----- 0 Config
01/11/07 06:45p d----- 0 Connection Wizard
01/11/07 11:34p -a----- 0 control.ini
01/11/07 11:02p d----- 0 Cursors
01/14/07 04:20p d----- 0 Debug
08/29/02 01:00p -a----- 2 desktop.ini
01/12/07 05:46p -a----- 178 DMCPUFG.LOG
01/11/07 11:32p d----- 0 Downloaded Progr
01/11/07 06:45p d----- 0 Driver Cache

```

▲ Type `dir` in the Recovery Console to display a list of all files and folders (directories) contained in the current folder

command to find out how to use other file commands, such as copy, delete and rename, if you need them.

If you're trying to fix a PC that freezes during bootup, you'll probably find the system service commands `disable` and `enable` to be handy. We've covered how to use them in our 'How to... Disable a device driver or system service' box on the previous page.

POWER TOOLS

Recovery Console has partition-management and system-file repair tools. Casual use of these could cause serious problems, but if you're considering using them it's likely that your PC is in real trouble and you've got little to lose.

A safe one to start with is `chkdsk`. If you run it without any additional parameters, it will launch a simple check of the current hard disk (or 'volume'), resulting in a report. For an exhaustive but slower check, try `chkdsk /p`. If the `chkdsk` report reveals problems, use `chkdsk /r` to

have Recovery Console mark bad sectors on the disk and recover readable data. This cures some startup problems. To erase all data from a drive or partition, use the format command. Entering `format c: /q /fs:ntfs`, for example, performs a quick format on drive letter C: and prepares it with the NTFS file system. Naturally, you'll lose any data still on the disk.

It is also possible to manage partitions in Recovery Console. To do this, type `diskpart` at the command-line prompt and hit Enter. The prompt will be replaced by a slightly more friendly interface that can be navigated using the cursor keys. Select an entry from the list and press C to create a new partition and follow the onscreen prompts, or D to delete the highlighted one. Deleting a partition is a one-way process; all the data stored on the partition will be lost. To exit this interface, press Escape.

If all that seems scary, take comfort in the fact that the Recovery Console has a few built-in fixing tools that require little specialist knowledge to use but can quickly repair an

apparently terminally ill PC. Run the `fixboot` command and a new partition boot sector will be written to the specified drive or partition. For example, to fix the C: drive you would run `fixboot c:`. This may resolve booting problems, even if you don't know what's wrong.

Similarly, if your PC fails to boot and you receive specific messages warning of a damaged master boot record, using the `fixmbr` command can help. This writes a new master boot record on to the boot device, which is normally the first hard disk. To find the name of all the available devices, type `map` and hit Enter. A list of all attached storage devices is displayed. If your boot drive is `\Device\HardDisk0`, use the command `fixmbr \Device\HardDisk0` to write a new master boot record to this device. This is something of a nuclear option, though – don't do this for fun. Writing a new master boot record to the primary partition could cause other partitions to become inaccessible.

When you've finished with the Recovery Console, simply type `exit` and hit Enter. **CS**

```

The following list shows the existing partitions and
unpartitioned space on this computer.

Use the UP and DOWN ARROW keys to select an item in the list.

  * To create a partition in the unpartitioned space, press C.
  * To delete the selected partition, press D.

16379 MB Disk 0 at Id 0 on bus 0 on atapi (MBR)
  25 Partitions (11703)  16379 MB (16226 MB free)

ESC=Cancel  D=Delete Partition

```

▲ The `diskpart` command can create or delete drive partitions from within the Recovery Console

```

The Recovery Console provides system repair and recovery functions.
Type EXIT to quit the Recovery Console and restart the computer.

1: C:\WINDOWS
Which Windows installation would you like to log onto
(C to cancel, press ENTER)? 1
Type the administrator password:
C:\WINDOWS\system32\cmd.exe
Volume created 01/14/07 05:43p
The volume Serial Number is 7052-c124

The volume appears to be in good condition and was not checked.
Use /p if you want to check the volume anyway.

16771828 kilobytes total disk space.
15591548 kilobytes are available.

4096 bytes in each allocation unit.
4122832 total allocation units on disk.
3897887 allocation units available on disk.

```

▲ Running the `chkdsk` command will display a report of the current or specified drive's health. Use the `/r` parameter to have Recovery Console mark bad sectors and rescue readable data

Lost for words Recovering a Windows XP administrator password

If you forget the administrator account password in Windows XP, you could be in real trouble. Windows XP doesn't provide an easy way to recover an administrator login for security reasons, which is sensible. However, it is possible to reset an administrator password in an emergency. Don't do this regularly, though, as it can cause problems.

The easiest and safest way is to use a tried and trusted commercial package that runs safely from within Windows XP itself. Elcomsoft's excellent Proactive Password Auditor can launch dictionary-based or so-

called 'brute force' attacks to reveal almost any password stored on the PC, including those for administrator accounts. However, this package is aimed at network administrators and costs £249 for a 20-user licence.

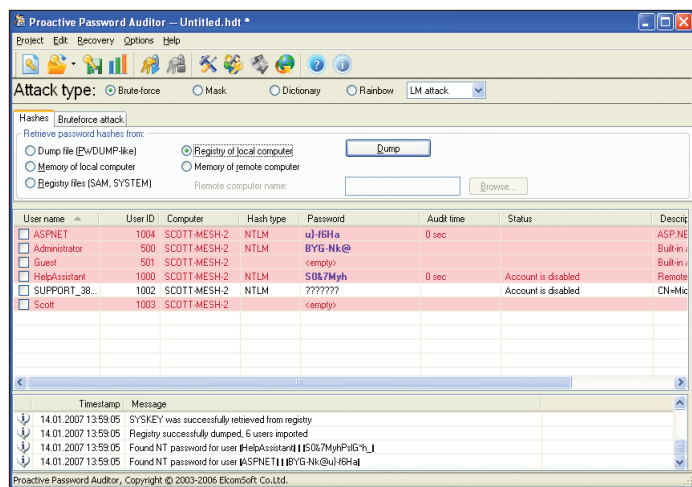
In the unlikely event that your PC is running Windows XP Service Pack 1 (SP1), there's a useful trick that exploits a security hole in XP, enabling anyone with access to the Windows XP installation to change the passwords for any user account (including administrator accounts). The method is too complicated to cover in detail here, but if you run a Google

search on 'security hole' and 'NUSRMGR.CPL' you'll see how to hack your own PC.

Most PCs should be running Windows XP SP2 by now, in which case the above security hole will be fixed. So it's back to the third-party software to reset the password. An affordable commercial package is Active Password Changer. This DOS-based utility boots from floppy disk or CD. Active Password Changer offers little more than the ability to reset local administrator and user passwords on Windows NT/2000/XP/Server 2003/Vista PCs, but it does it reliably and it's also affordable, costing US\$40 (around £20) from www.password-changer.com.

For the budget-conscious or brave (or both), we suggest a Linux-based password-cracking tool such as Ophcrack LiveCD. This bootable-CD version of the Linux operating system can be used to reveal Windows XP password 'hashes' without going anywhere near Windows or the Recovery Console. It's free, but less easy to use than the commercial options mentioned. You can download it from <http://ophcrack.sourceforge.net>.

Regardless of which route you take, using tools to reset an administrator password may cause encrypted files and folders, or other data and network shares, to become inaccessible. We therefore recommend doing this only if absolutely necessary and, even then, with great caution. Read, read and read again the supplied instructions.



▲ Use third-party commercial software packages or open-source freeware tools to sniff out and display almost any password stored on a Windows XP computer